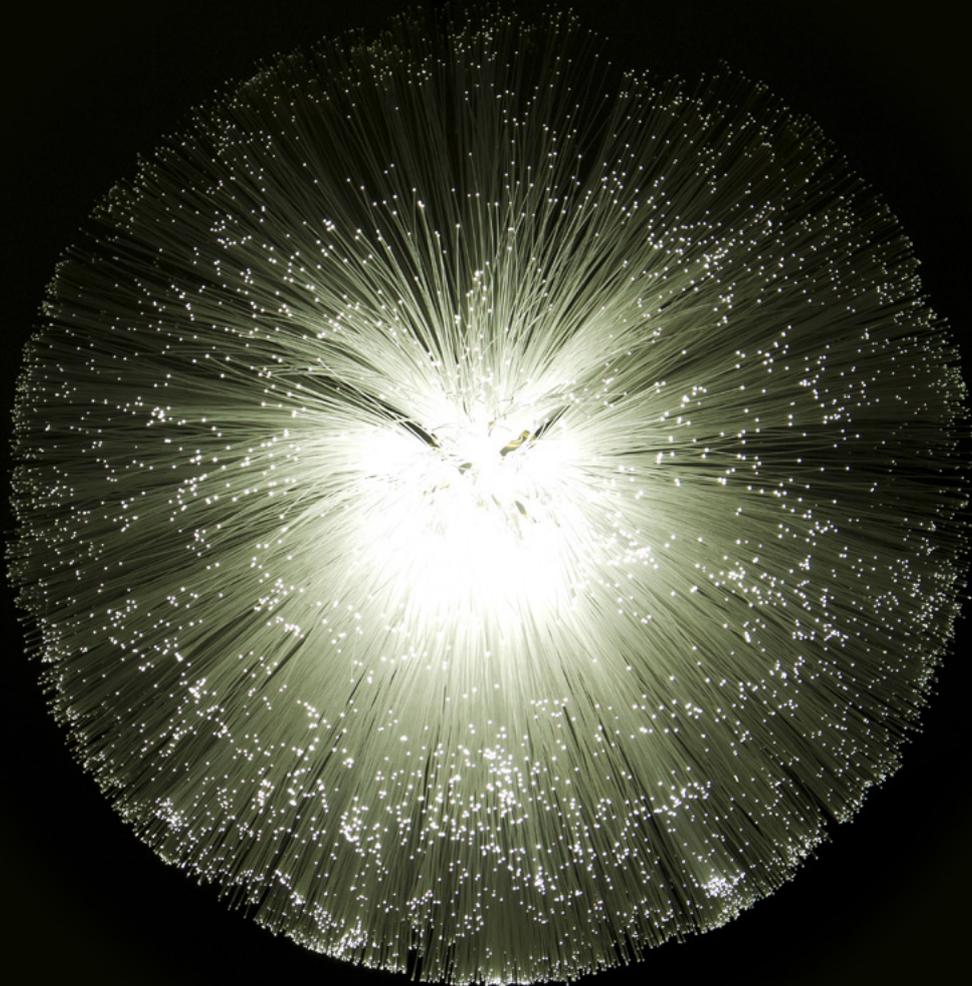


**Deloitte.**



**Under the spotlight**  
Data Integrity in life sciences

# Introduction

Summary	3
What is Data Integrity?	4
Why is there a focus on Data Integrity compliance by regulators?	6
What are the key challenges companies face when implementing Data Integrity best practices?	8
Common Data Integrity Violations	9
What are the consequences if Data Integrity is failing?	10
Approach to Data Integrity compliance	11
Conclusion	13
References	14
Contacts	15

# Summary

The integrity of data generated by highly regulated life sciences companies is critical, because properly recorded information is the basis for manufacturers to assure product quality, safety and efficacy prior to product approvals and subsequently placing them onto the markets for human use.

Data Integrity is also important for quality control procedures during manufacturing to ensure patient safety. As global regulatory focus on Data Integrity increases, companies that fail to comply may face penalties ranging from public warning letters to criminal charges and product removal from the marketplace. In recent years there has been a significant increase in the number and types of issues related to data practices, including: unauthorized data access, lack of enabled audit trails, accidental and intentional falsification of records.

Regulatory bodies now have high expectations with regard to data quality and integrity owing to the life sciences industry's growth, globalization and adoption of advanced technology, such as highly automated systems and storage of data in 'The Cloud'. The need to be compliant is expected to drive organizations to make significant changes to their current data-related processes and systems that require corporate-wide efforts and cross-functional collaborations. The implementation of good data practices requires consideration, not just of controls, processes, IT and clear roles and responsibilities, but of a wider shift towards education and a culture that understands and values Data Integrity.

# What is Data Integrity?

According to the guidelines published by the regulatory bodies, Data Integrity is defined as the extent to which all data are complete, consistent, and accurate throughout the data lifecycle. Data here includes all original records and true copies, including source (raw) data, metadata and all subsequent transformations and reports of these data.<sup>1,2,3,4,5</sup>

Regulatory authorities expect paper and electronic data generated in the process of testing, licensing, manufacturing, packaging, distribution, and monitoring of medicines to be collected and maintained in a secure manner. The requirements for data include that they are attributable, legible, contemporaneous, original and accurate (ALCOA) (Figure 1).

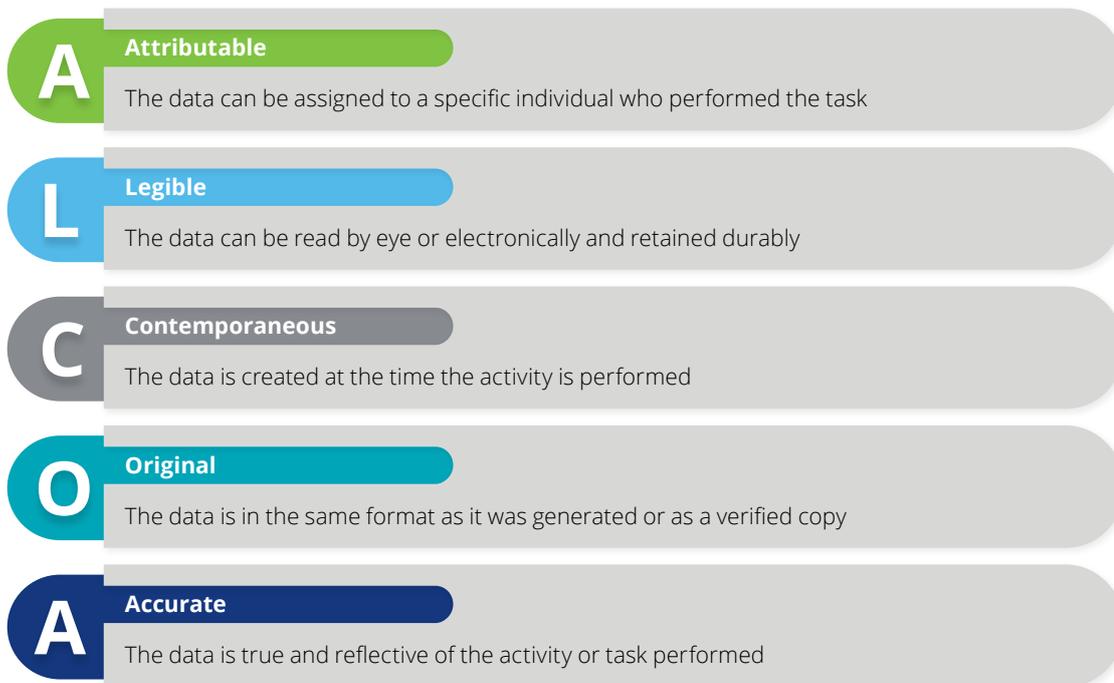


Figure 1: ALCOA characteristics of data

Implicit in the requirements for ALCOA are that data should be complete, consistent, enduring and available (usually referred to as ALCOA+).

In addition to ALCOA, there are standards for storage and backup, which must be applied equally to both electronic and paper-based data. Where paper data exists, it must be stored and backed up as securely as electronic data. Scanning paper data elements for backup is good practice, but must be performed utilizing a validated process and controlled by verification of completeness. Where data retention is outsourced to an external party, the elements of the contract which relate to ownership and retrieval of data should be thoroughly understood, and the vendor should be qualified and managed like any other critical services vendor through established vendor management processes. It is important to realize that data are part of the Good Manufacturing Process (GMP) supply chain and must be treated with the same standards of quality.

The different guidelines produced by the various regulators are substantially harmonized with each other. Therefore, changes to data life-cycle management performed in order to comply with one of the guidelines automatically facilitates compliance with the other guidelines.

From the generation and processing of data to its storage and destruction, there are many components that contribute to compliance with regulations and international standards. Maintaining a high level of Data Integrity is multifaceted and requires not only strong policies and controls, but also staff training, segregation of duties and a culture of compliance. A typical data lifecycle beginning with the creation of data and ending in its deletion is shown in Figure 2 along with good data practices for each phase.<sup>6</sup>



Figure 2: Typical data lifecycle and good practices for each stage

# Why is there a focus on Data Integrity compliance by regulators?

During GMP inspections by regulators a number of violations in data manipulation and other data issues were identified in pharmaceutical manufacturing facilities, particularly ones based in Asia.<sup>7,8</sup>

In 2016, a regulatory agency issued 75 warning letters for a range of violations including unlawful promotion, insufficient registration, unlawful distribution, scientific violations and manufacturing quality violations. Of these letters, 43 per cent contained instances of Data Integrity violations (Figure 3).<sup>9</sup>

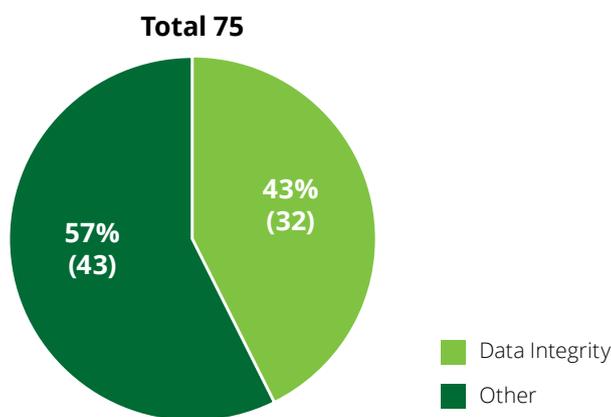


Figure 3: Percentage of total FDA warning letters issued in 2016

These warning letters were heavily skewed towards manufacturers in Asia, which accounted for 72 per cent of 32 data related warning letters issued globally, with the remainder being spread across Europe and Americas (Figure 4).<sup>10</sup>

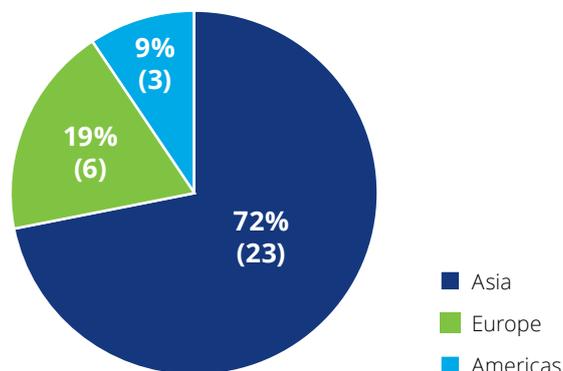


Figure 4: Data Integrity related warning letters issued in 2016 by the regulatory agency

The relevant warning letters were issued for a range of different reasons, most commonly due to data not being fully and accurately documented, which accounted for 34 per cent of the violations (Figure 5).<sup>11</sup>

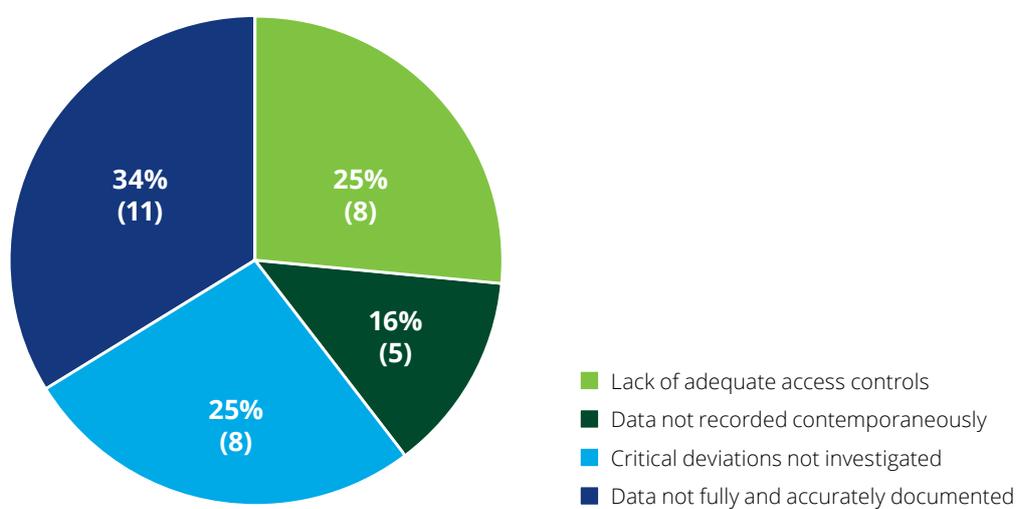


Figure 5: Breakdown of the 32 Data Integrity violations brought up in warning letters in 2016

Due to such frequent violations of basic Data Integrity practices, regulators globally are focusing on enforcing principles and practices to ensure product quality and patient safety.

# What are the key challenges companies face when implementing Data Integrity best practices?

There are a range of challenges faced by life science organisations attempting to implement good data practices.

These include:

- Challenges to embedded quality and data integrity into an organisational culture – Most companies understand the need for a data quality culture but do not know how to implement it. ‘Everyone is responsible for quality’. Creating a culture of quality through design and duty is the key to data quality and integrity. Leading, training and empowering employees to take ownership and responsibility of quality in their day-to-day working fosters a good quality culture and improves Data Integrity and transparency.
- Limited awareness and appropriate levels of training – A good culture can only be fostered and maintained if employees are given the right resources to operate efficiently and effectively. It is important to assess and understand the type and level of training needs across the organisation in order to ensure productivity. In a competitive world, all employees are expected to deliver more in less time. As a result, in some instances increased performance pressures mean that employees cut corners and try to deliver in time by compromising quality and indirectly influencing Data Integrity. Employees should be made aware of the true costs of failing data quality and its impact to patients.
- Insufficient controls and inefficient business processes/ systems – In order to embed data quality and Data Integrity in organisational culture, companies must implement quality systems, defined business processes and robust controls. This will ensure that the data lifecycle is optimised and data is generated in a consistent and timely manner without compromising data quality.
- Contracting or outsourcing work to a third party vendor – If a life sciences company currently outsources work to another third party, the company has the responsibility to ensure the adequacy of data and comparable systems used by the third party vendor. This also applies to data maintained by a third party and examples include contracted IT data centres, database support personnel and cloud computing solutions. The responsibility of an organisation to maintain Data Integrity across its extended enterprise can provide significant challenges in the assurance and monitoring of data quality.
- Data volumes and complexity – Data volumes in the life sciences industry are growing exponentially coming from a variety of data sources. Data is sourced, manipulated and surfaced in numerous ways resulting in varying confidence in data quality and reliability. With the growth in the amount of available data, companies are struggling with interpreting, analysing and converting data in to meaningful insights. The explosion in the volume and complexity of data about medicines, patients, processes and operations reveals data integrity risks in areas that were previously considered safe. Without data that is consistent, accurate and reliable across the enterprise, an organisation can become less competitive, and less efficient.

# Common Data Integrity Violations

As part of their standard inspection process, regulatory agencies verify the accuracy and integrity of various data, with an increasing focus on quality control activities. As discussed above, a number of recent warning letters have highlighted such concerns. Issues noted in these letters encompass many of the elements highlighted in recent guidance. These issues include, and are not limited to, the following:

- *“Failure to maintain complete data derived from all laboratory tests conducted to ensure compliance with established API specifications and standards.”* In the example, this failure included the discovery of residual solvent testing data in the Recycle Bin folder, and failure to retrieve test data upon request.<sup>12</sup>
- *“Failure to prevent unauthorized access or changes to data, and failure to provide adequate controls to prevent omission of data.”* This failure, in one case, included the discovery that chromatography metadata (e.g. time and date) could be changed without the changes being reflected in the audit trail. In another case, analysts deleted unknown peaks without justification, making the drugs in question appear to conform to their specifications. One of these peaks was for a residual solvent known to be a genotoxic impurity.<sup>13</sup>
- *“Failure to record activities at the time they are performed and destruction of original records.”* In one case, this failure involved the backdating of batch production records, and the destruction of original records after being manually transcribed.<sup>14</sup>
- *“Failure to train employees on their particular operations and related GMP practices.”* In the example, this included the declaration by employees that they had not received training for their production operations. The company in question was not able to produce any training reports for inspectors, despite the generation of training reports being part of company policy.<sup>15</sup>

# What are the consequences if Data Integrity is failing?

As noted above, following recent GMP inspections, violations and failures have resulted in a range of regulatory actions, including warning letters, import alerts and product detentions. Current guidance indicates that failures in Data Integrity can result in the following regulatory and non-regulatory consequences<sup>16</sup>:

- Frequent inspections or suspension of product approvals - when regulatory issues arise, they are likely to result in loss of regulatory trust. This can result in more frequent inspections of the facility, a requirement to see more data to support claims, and may make it unlikely for a company to obtain approvals from the regulatory authority.<sup>18</sup>
- Import bans, forced recalls, plant shutdowns, debarment - for serious violations, products which have Data Integrity issues are considered by the regulatory agency to be adulterated. As such, if they are shipped to the USA, the regulatory agency can prevent them from being allowed into the country. Additionally, they can mandate that the product be recalled or subject to seizure. Health Canada has also imposed restrictions, quarantines and recalls due to Data Integrity concerns based on the findings of other regulatory bodies. The regulatory body can, at its own discretion, punish even technical violations which may not result in obvious threats to patient health. In addition to warning letters, the available enforcement actions include approval withdrawals, plant shutdowns, injunctions or penalties and debarment of individuals. The regulatory body has also resorted to suspending drug sales when it discovered that the integrity of the underlying data was compromised.<sup>19,20,21</sup>
- Criminal enforcement - the New England Compounding Centre manufactured drug products that resulted in a number of individuals dying from meningitis. During an inspection by a regulatory agency, the investigators found numerous cases of negligence and Data Integrity issues, for example, falsified cleaning logs to show cleaning was performed when it was not performed. Following the investigation, criminal charges were filed against 14 employees from high level executives to operators in the clean room. Conviction on these types of charges can result in prison terms in addition to large fines.<sup>22</sup>
- Loss of reputation and public trust - the publication of warning letters in newspapers and consumer domains, can significantly tarnishes the reputations of a company. This may result in a loss of public confidence in those companies affected and lead to a loss of business. There have recently also been high profile warning letters from the regulatory body for serious GMP violations which can result in adverse publicity.<sup>23</sup>
- Lack of strategic data insights - the industry is seeing a push towards using generated data not just for regulatory compliance and quality assurance, but moreover to gain strategic insights into their businesses. Weak standards of Data Integrity will compromise the potential of an organisation to generate value and a competitive advantage through data driven decision making.

# Approach to Data Integrity compliance

Cross-functional collaboration and integrated systems and processes are the key evolving trends that are becoming evident as life sciences companies adapt to the changing regulatory landscape to achieve compliance. The upcoming regulations require companies to make significant changes to their systems and processes, thereby changing the ways of working. Companies need to ensure that they have appropriate levels of controls and measures in place to create consistent, accurate and quality data with minimal disruption. These measures apply to both manual and electronic data generation and should be commensurate with differing levels of risk.

Data Integrity requires a cohesive, integrated, cross-functional and company-wide programme in order to succeed. Working in silos can lead to inefficiencies, gaps, poor data quality and insufficient security across the product lifecycle. A focus on building a quality embedded organisational culture, assessing risk appetite and maturity, understanding procedures and standards, optimising technology and system capabilities as well as aligning and integrating governance framework will be essential (Figure 6).

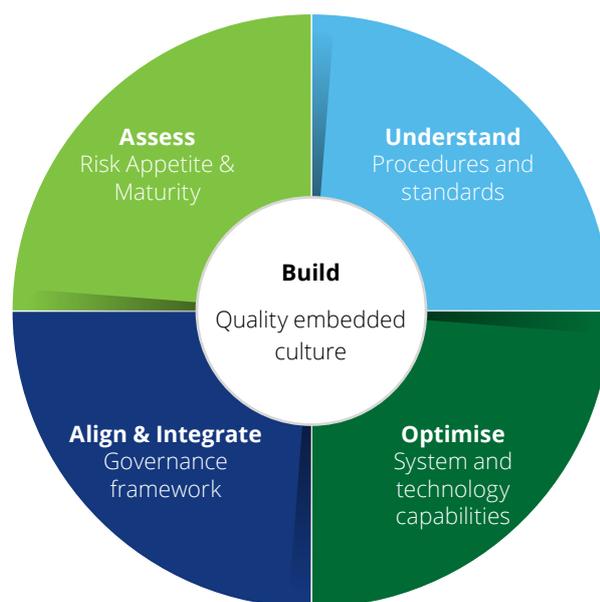


Figure 6: Approach to implementing Data Integrity across an organisation

## Building a quality embedded culture

There is a link between data quality, Data Integrity and business culture. The diagram below highlights what a quality embedded culture could look like (Figure 7). Regulators now expect the industry to be proactive in its efforts to implement good Data Integrity practices, rather than just react to inquiries or defend themselves if audited. This should promote the creation of a working environment that encourages an open reporting culture. Companies also need to understand the impacts that their decisions and actions may have on the products and subsequently patient safety if they ignore Data Integrity issues.

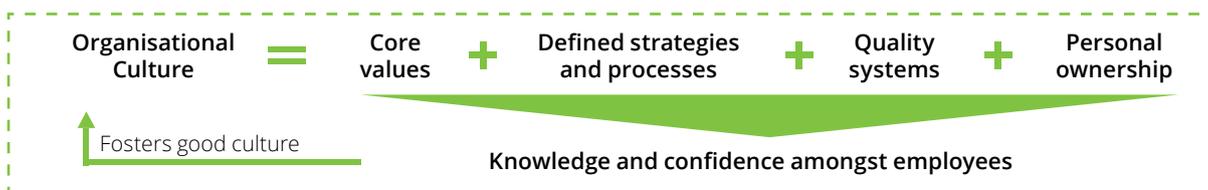


Figure 7: The scheme of a quality embedded culture

In order to build and implement a quality culture, companies should focus on the following:

- Incorporate quality as part of your company's core values
- Provide a written code of conduct that will guide and empower your employees and contractors to deliver quality in business as usual tasks, including data collection, processing and management
- Create strong peer groups within the organisation that will guide employees when in doubt
- Build knowledge and awareness on the importance of quality to the organisation and ultimately to the patients
- Reward employees when they report quality issues and make quality and Data Integrity a priority

#### Assess risk appetite and maturity

Define the level of risk your company can accept and the standards you need to achieve. Conduct a maturity gap analysis of business processes, systems and data against the regulatory requirements. Use risk assessment techniques such as ICH Q9 Quality Risk Management to determine the importance of each data processing step by effectively monitoring data criticality and data risk including impact of alteration on data vulnerability, product quality and safety at each stage of the data lifecycle. When analysing the identified risks, the focus should be on reviewing the current controls of data in a process, procedure or a system in order to identify any weaknesses and minimise the risks.

#### Understand the procedures and standards

Review and analyse available regulatory documents including official regulations, industry guidance and definitions from leading regulatory bodies to define common data integrity standards and procedures. These regulatory documents should be interpreted and implemented into an organisation's business processes, procedures and policies. Process optimisation, including contracting processes for third party obligations, should be at the forefront when implementing a Data Integrity programme.

#### Optimise system and technology capabilities

Data Integrity concerns should be tackled as part of a broader technology risk management strategy that addresses data security, application controls, cyber risk and IT operational management. This will help strengthen and optimise the existing IT landscape. A RACI should be defined along with access privileges including unique logins to enable the audit trail function that records all actions taken by each person. Audit trails should be reviewed at pre-defined intervals that are commensurate with differing levels of risk. It is important to recognise that data relating to a product or process may cross various boundaries during their lifecycle and companies will need to further assure that their products have been manufactured according to recognised and validated protocols and that all related information is traceable, recorded and reported whilst maintaining Data Integrity at all times.

#### Align and integrate governance framework

Define and deliver a Data Integrity strategy and governance framework that will define the principles for managing and maintaining Data Integrity within the organisation. Create a governance committee at a global level to monitor practices within the organisation and throughout the extended enterprise, including third party contractors. The governance framework should take into account the entire data lifecycle and address data ownership, design, operation, review and monitoring of data-related processes. At local levels, subject matter experts should provide specific advice and recommendations for improvement opportunities. All the process and system owners should be responsible for monitoring and reporting on their Data Integrity performance within the organisation.

# Conclusion

The growing issues of Data Integrity across life science companies means that organisations need to be able to adapt rapidly to prevent violations and regulatory consequences. Good data practices will enrich the quality of data, allowing companies to make strategic decisions backed by analytics and data-driven insights. To enable this, companies will need to provide sufficient training to their employees, develop assessment and monitoring programmes, as well as establish Data Integrity as an integral part of the internal audit programme. Such changes are essential to developing a culture that values data quality with an awareness of and focus on GMP. Companies that fail to develop and implement suitable standards risk falling behind global regulatory requirements and may face consequences ranging from recalls and plant shutdowns to criminal charges, in addition to losing the competitive advantage of valuable data insights.

# References

1. [http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/q\\_and\\_a/q\\_and\\_a\\_detail\\_000027.jsp&mid=WC0b01ac05800296ca#](http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/q_and_a/q_and_a_detail_000027.jsp&mid=WC0b01ac05800296ca#)
2. <http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM495891.pdf>
3. [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/538871/MHRA\\_GxP\\_data\\_integrity\\_consultation.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/538871/MHRA_GxP_data_integrity_consultation.pdf)
4. <https://picscheme.org/en/news?itemid=33>
5. [http://www.gmp-compliance.org/guidemgr/files/WHO\\_TRS\\_996\\_ANNEX05.PDF](http://www.gmp-compliance.org/guidemgr/files/WHO_TRS_996_ANNEX05.PDF)
6. [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/538871/MHRA\\_GxP\\_data\\_integrity\\_consultation.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/538871/MHRA_GxP_data_integrity_consultation.pdf)
7. India's Data Integrity Problems, RAPS 03 February 2015
8. US FDA Inspections in China: An Analysis of Form 483s from 2015, RAPS 10 February 2016
9. <http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/EnforcementActivitiesbyFDA/WarningLettersandNoticeofViolationLetterstoPharmaceuticalCompanies/ucm482462.htm>
10. Ibid
11. Ibid
12. <http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2016/ucm528590.htm>
13. Ibid
14. <http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2015/ucm455345.htm>
15. Ibid
16. <http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM495891.pdf>
17. Ibid
18. Data Integrity in Pharmaceutical Industry: Journal of Analytical & Pharmaceutical Research 2016, 2(6): 00040
19. <http://www.hc-sc.gc.ca/dhp-mps/pubs/compli-conform/tracker-suivi-eng.php>
20. <https://www.dlapiper.com/en/us/insights/publications/2016/05/the-writings-on-the-wall/>
21. <http://www.fdanews.com/topics/111-data-integrity>
22. 14 Indicted in Connection with New England Compounding Center and Nationwide Fungal Meningitis Outbreak Wednesday, Department of Justice, Office of Public Affairs December 17, 2014.
23. <https://www.bloomberg.com/news/articles/2017-01-24/shredding-paper-before-fda-visit-raises-india-compliance-queries>

# Contacts

## David Hodgson

### Partner

DTTL Global LSHC Risk Advisory Leader  
davhodgson@deloitte.co.uk

## Fiona Maini

### Director

Deloitte UK  
fmaini@deloitte.co.uk

## William Greenrose

### Advisory Managing Director

Deloitte United States  
wgreenrose@deloitte.com

## Sinja Christiani

### Director

Deloitte Switzerland  
sichristiani@deloitte.ch

## Sarah Chan

### Senior Manager

Deloitte UK  
sachan@deloitte.com

## Balazs Hargitai

### Assistant Manager

Deloitte Switzerland  
bhargitai@deloitte.ch

## Acknowledgements

Gagan Arora

Jai Dongre

Namita Pai

Federico Negri



Other than as stated below, this document is confidential and prepared solely for your information and that of other beneficiaries of our advice listed in our engagement letter. Therefore you should not, refer to or use our name or this document for any other purpose, disclose them or refer to them in any prospectus or other document, or make them available or communicate them to any other party. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). In any event, no other party is entitled to rely on our document for any purpose whatsoever and thus we accept no liability to any other party who is shown or gains access to this document.

© 2017 Deloitte LLP. All rights reserved.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom.

Deloitte LLP is the United Kingdom member firm of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee, whose member firms are legally separate and independent entities. Please see [www.deloitte.co.uk/about](http://www.deloitte.co.uk/about) for a detailed description of the legal structure of DTTL and its member firms.